

1 CLAIMS:

2 What is claimed, is:

3 (1) A communications monitoring system comprising:

4 a communications sensor for receiving communications packets
5 flowing at arbitrary points on a network; and

6 a similarity calculator for calculating formal similarity
7 between two packet streams composed of communications
8 packets entering the sensor upon arrival of the
9 communications packets.

10 (2) The communications monitoring system according to Claim
11 1, wherein the similarity calculator represents the two
12 packet streams by graphs depicting amounts of data in
13 communications packets in respective packet streams with
14 respect to elapsed time, and calculates similarity between
15 the two packet streams based on size of regions enclosed by
16 the two graphs when the graphs of the packet streams are
17 moved close to each other without intersecting each other.

1 (3) The communications monitoring system according to Claim
2 1, wherein the communications sensor sends out a
3 predetermined alert according to a similarity value
4 calculated by the similarity calculator.

5 (4) A communications monitoring system comprising:

6 a packet input means for receiving communications packets
7 flowing at arbitrary points on a network; and

8 matching means for performing real-time matching between two
9 packet streams composed of communications packets received
10 by the packet input means.

11 (5) The communications monitoring system according to Claim
12 4, wherein the matching means determines formal similarity
13 between the two packet streams based on a time lag between
14 each corresponding pair of communications packets in the two
15 packet streams.

16 (6) The communications monitoring system according to Claim
17 5, further comprising alerting means for sending out a
18 predetermined alert according to the formal similarity

1 between the two packet streams determined by the matching
2 means.

3 (7) A communications monitoring method for monitoring data
4 communications using a computer, comprising the steps of:

5 acquiring communications packets in sequence from arbitrary
6 points on a network and storing them in predetermined
7 storage means together with information about a packet
8 stream to which the communications packets belong;

9 on reception of a predetermined communication packet, taking
10 another communications packet received within a
11 predetermined time before acquiring a predetermined
12 communications packet, out of the storage means;

13 determining formal similarity between the first packet
14 stream which contains up to the acquired communications
15 packet and a second packet stream to which the
16 communications packet taken out of the storage means belong;
17 and

18 sending out a predetermined alert according to the
19 determined similarity.

1 (8) The communications monitoring method according to Claim
2 7, wherein in the step of determining the formal similarity
3 of packet streams, the formal similarity between the two
4 packet streams is determined based on a time lag between
5 each corresponding pair of communications packets in the two
6 packet streams.

7 (9) The communications monitoring method according to Claim
8 7, further comprising a step of discarding information used
9 in determining the similarity of second packet streams
10 except the second packet stream determined to be most
11 similar to the first packet stream.

12 (10) An information processing method comprising comparing
13 two packet streams flowing on a network, the step of
14 comparing comprising the steps of:

15 acquiring communications packets in sequence from arbitrary
16 points on a network and storing them in predetermined
17 storage means together with information about a packet
18 stream to which the communications packets belong;

19 on reception of a predetermined communication packet, taking

1 another communications packet received within a
2 predetermined time before acquiring a predetermined
3 communications packet, out of the storage means; and

4 performing matching between the first packet stream which
5 contains up to the acquired communications packet and a
6 second packet stream to which the communications packet
7 taken out of the storage means belong.

8 (11) The information processing method according to Claim
9 10, wherein in the step of performing matching between the
10 packet streams, the first and second packet streams are
11 represented by graphs which depict increments of sequence
12 numbers of communications packets in respective packet
13 streams with respect to elapsed time and the similarity
14 between the two packet streams is calculated based on size
15 of regions enclosed by the two graphs when the graphs of the
16 packet streams are moved close to each other without
17 intersecting each other.

18 (12) The information processing method according to Claim
19 11, wherein in the step of calculating the similarity
20 between the packet streams, information used in determining
21 the similarity is discarded according to time-axis lengths

1 of the regions enclosed by the two graphs.

2 (13) An article of manufacture comprising a computer usable
3 medium having computer readable program code means embodied
4 therein for causing communications monitoring, the computer
5 readable program code means in said article of manufacture
6 comprising computer readable program code means for causing
7 a computer to effect the steps of claim 7.

8 (14) A program storage device readable by machine, tangibly
9 embodying a program of instructions executable by the
10 machine to perform method steps for communications
11 monitoring, said method steps comprising the steps of claim
12 7.

13 (15) An article of manufacture comprising a computer usable
14 medium having computer readable program code means embodied
15 therein for causing information processing, the computer
16 readable program code means in said article of manufacture
17 comprising computer readable program code means for causing
18 a computer to effect the steps of claim 10.

19 (16) A program storage device readable by machine, tangibly
20 embodying a program of instructions executable by the

1 machine to perform method steps for information processing,
2 said method steps comprising the steps of claim 10.

3 (17) A computer program product comprising a computer usable
4 medium having computer readable program code means embodied
5 therein for causing communications monitoring, the computer
6 readable program code means in said computer program product
7 comprising computer readable program code means for causing
8 a computer to effect the functions of claim 1.

9 (18) A computer program product comprising a computer usable
10 medium having computer readable program code means embodied
11 therein for causing communications monitoring, the computer
12 readable program code means in said computer program product
13 comprising computer readable program code means for causing
14 a computer to effect the functions of claim 4.